AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Jeffrey Plank, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain cellular towers ("cell towers") that are in the possession, custody, and/or control of Verizon Wireless, a cellular service provider headquartered in Basking Ridge, New Jersey; T-Mobile US, Inc., a cellular service provider headquartered in Parsippany, New Jersey; and AT&T Corporation, a cellular service provider headquartered in North Palm Beach, Florida. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Verizon Wireless, T-Mobile US, Inc., and AT&T Corporation to disclose to the government the information further described in Section I of Attachment B, government-authorized persons will review the information to locate items described in Section II of Attachment B.

2. I am Sergeant Jeffrey Plank, working for the Utah State Bureau of Investigation (SBI), under the Utah Department of Public Safety (DPS) and am currently assigned as a Task Force Officer to the Cyber Squad of the FBI Salt Lake City Field Office in the District of Utah. I was deputized as a federal task force officer in July of 2013. I have been employed with DPS since July 1998, which included three months of training at the Police Officer Standards and Training in Sandy, UT.

3. I have received training presented by Drug Enforcement Administration, Utah Crime Lab, Utah Office of Medical Examiner's Office, Utah Attorney General's Office, Rocky

Mountain High Intensity Drug Traffic Area, Utah Narcotic Officer's Association, FBI LEEDA, Homeland Security, Department of Justice, Public Agency Training Council, the Office of National Drug Control Policy, SANS Institute, New Horizons Computer Learning Center, and Utah Organized Retail Crime Association. The training includes marijuana eradication, clandestine laboratory investigation, drug intelligence analysis, indoor marijuana cultivation, narcotics investigations, identity theft, death investigations, evidence handling, asset forfeiture, money laundering, identification of fraudulent documents, crimes using handheld devices, cell phone investigations, forensic interview training, DNA crime scene collection and CompTIA A+, CompTIA Net+, SANS 301, SANS 401 and organized retail theft crime. I have also earned a master's degree in Cybersecurity and Information Assurance from Southern Utah University.

4. The facts in this affidavit come from information obtained from my investigation, training, experience, and information obtained from other agents and witnesses. This affidavit is intended only to show that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

5. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1030 (computer fraud) and 18 U.S.C. § 2113(b) (bank fraud) have been committed by unknown persons. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), &

(c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

7. In February 2024, the Salt Lake City Federal Bureau of Investigation (FBI) Cyber Squad was informed by the Salt Lake City Community College that an ATM Jackpotting operation occurred on their campus located at 4600 S Redwood Rd, Salt Lake City, UT. Video surveillance shows that on February 6, 2024, unidentified subjects stole approximately $56,000 from the ATM. Subjects who obtained cash from the ATM were seen on surveillance video on February 6, 2024 between 9:00 A.M. and 2:10 P.M accessing the ATM and or standing or sitting near it.

8. ATM Jackpotting can be performed in one of two different ways. Either the criminal uses malware which sends commands to the dispenser, or they use their own "black box" hardware device connected directly to the dispenser to cash-out the ATM.

9. Malware jackpotting attacks typically happen in two phases. First, the criminal prepares the ATM by infecting it with malware. This can be done remotely via access to remote software distribution, for example, or on-site, typically with a USB mass storage device. The jackpotting malware can then sit silently, waiting in the ATM undetected while normal ATM transactions take place. The second phase occurs when the criminal visits the ATM and triggers the dispense command.

10. Depending on the jackpotting malware used, the dispense command can be initiated with a preconfigured card, the entry of a special PIN, or the use of a keyboard. Black box attacks involve the disconnection of the ATM dispenser from the ATM PC. An external black box device such as a laptop or tablet is then connected and fraudulently re-paired with the

dispenser, enabling the laptop or tablet to send cash-out commands directly to the cash dispenser. The majority of these jackpotting attacks involve some physical access to the ATM.

11. In February of 2024, surveillance video of the Jackpotting was provided to the FBI and reviewed. Surveillance video showed that approximately eight subjects, wearing masks and glasses, were working as a crew and taking turns withdrawing cash from the ATM. Video surveillance actually shows this same crew attempting to "Jackpot" the same ATM on January 31, 2024 but appear to have not succeeded in obtaining any money from the ATM. Prior to obtaining cash from the ATM, members of this same crew were captured on video surveillance opening the ATM machine and accessing the ATM's computer hardware.

12. The hard drive from the ATM was seized and analyzed by the FBI. An analysis showed that a thumb drive containing malware had been inserted into the hard drive on January 31, 2024, February 2, 2024, and February 6, 2024, at the same time that members of this crew are on video opening the ATM. Files of interest on the hard drive are known malicious files frequently used in these kinds of Jackpotting cases known as Ploutus D. This malware allows an individual to remotely send commands to the ATM's hard drive to dispense cash. Based on video surveillance and what is known of Ploutus D, it is apparent that a subject sitting on the couch across from the ATM used a device to dispense cash while members of the crew were taking turns standing at the ATM to retrieve the dispensing cash.

13. While arranging to obtain the ATM hard drive from representatives of Diebold Nixdorf, the company that owns, maintains, and has access to surveillance video for the ATM, your affiant was informed that it appeared the same group may have targeted another ATM on the Southern Utah University campus (SUU).

14. On February 8, 2024, four masked individuals were captured on surveillance video at SUU, located at 351 W Center St, Cedar City, UT, withdrawing funds from an ATM between 4:16 P.M and 6:12 P.M. At least one of these subjects is also seen two days earlier on the Salt Lake Community College campus withdrawing cash from the ATM there. The individuals also used helium balloons to obscure the surveillance camera's view of the ATM. The hard drive for the SUU ATM was also recovered.

15. Based on your affiant's experience investigating and analyzing phones of arrested "jackpotters," and speaking with United States Secret Service agents who regularly work these cases, the individuals involved in the thefts described above likely communicated with each other using cellular devices, like smartphones, through telephone calls, text messages, or other forms of electronic communication. In addition, cellphones are often used as global position systems (GPSs) or navigation systems and may have been used to help the unknown suspects locate the addresses of the targeted ATMs. Cellphone tower information from the towers closest to the Salt Lake Community College and Southern Utah University will be requested to try and identify the subjects.

16. Based on your affiant's training and experience, there is a high probability that even if the subjects did not contact each other while the ATMs were attacked, the subjects would still have had their cellphones on their persons, which could be used to show that they were on campus.

17. Wireless providers such as Verizon Wireless, T-Mobile US, Inc., and AT&T Corporation are companies that provide cellular communications services to the general public. Your affiant knows that in order to provide these services, many cellular service providers maintain antenna towers (cell towers) that serve and provide cellular service to devices that are

within range of the tower's signals. Each cell tower receives signals from wireless devices, such as cellular phones, in its general vicinity. By communicating with a cell tower, a wireless device can transmit and receive communications, such as phone calls, text messages, and other data. When sending or receiving communications, a cellular device does not always utilize the cell tower that is closest to it.

18. Based on your affiant's training and experience, each cellular device is identified by one or more unique identifiers. For example, with respect to a cellular phone, the phone will be assigned both a unique telephone number but also one or more other identifiers such as an Electronic Serial Number (ESN), a Mobile Electronic Identity Number (MEIN), a Mobile Identification Number (MIN), a Subscriber Identity Module (SIM), a Mobile Subscriber Integrated Service Digital Network Number (MSISDN), an International Mobile Subscriber Identifier (IMSI), or an International Mobile Equipment Identity (IMEI). The types of identifiers assigned to a given cellular device are dependent on the device and the cellular network on which it operates.

19. Your affiant knows that cellular providers, such as Verizon Wireless, T-Mobile US, Inc., and AT&T Corporation, routinely, and in their regular courses of business, maintain historical records that allow them to determine which wireless devices used cellular towers on the cellular provider's network to send or receive communications. For each communication sent or received via the wireless provider's network, these records may include: (1) the telephone call number and unique identifiers of the wireless device that connected to the provider's cellular tower and sent or received the communication ("the locally served wireless device"); (2) the cellular tower(s) on the provider's network, as well as the "sector" (i.e., face of the tower), to which the locally served wireless device connected when sending or receiving the

communication, and (3) the date, time and duration of the communication. These records may also include the source and destination telephone numbers associated with the communication (including the number of the telephone that was called or that called the locally served wireless device) and the type of communication (e.g., phone call or SMS text message) that was transmitted.

20. Based on my training and experience, I know that cellular providers, such as Verizon Wireless, T-Mobile, Inc., and AT&T Corporation, have the ability to query their historical records to determine which cellular device(s) connected to a particular cellular tower during a given period of time, and to produce the information described above. I also know that cellular providers have the ability to determine which cellular tower(s) provided coverage to a given location at a particular time.

21. Information obtained from cellular service providers such as Verizon Wireless, T-Mobile US, Inc., and AT&T Corporation, that reveals which devices used a particular cell tower (and, where applicable, sector) to engage in particular communications can be used to show that such devices were in the general vicinity of the cell tower at the time the communication occurred. Thus, the records described in Attachment A will identify the cellular devices that were in the vicinity of the ATMs at the times that the machines were attacked. This information, in turn, will assist law enforcement in helping determine which persons were present for each ATM attack as well as identify all members of the Jackpotting crew present not caught on camera. Since the same group of people will most likely have been present at both locations it should be easy to filter the results of the data for both locations and identify all those who were involved in the Jackpotting. The specific locations described in Attachment A are listed below.

- 4600 S Redwood Rd, Salt Lake City, UT on February 6, 2024, between 09:00 AM and 2:10 PM MST.
- 351 W Center St, Cedar City, UT on February 8, 2024, between 4:16 PM and 6:12 PM MST.

22. To protect information related to innocent third parties, the government will seize only information relevant to devices that used more than one of the cell towers that provided cellular service to the location specified in Attachment A during the time frames specified in Attachment A.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

23. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Verizon Wireless, T-Mobile US, Inc., and AT&T Corporation to disclose to the government copies of the records particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

24. Based on the forgoing, I request that the Court issue the proposed search warrant.

25. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Verizon Wireless, T-Mobile US, Inc., and AT&T Corporation. Because the warrant will be served on Verizon Wireless, T-Mobile US, Inc., and AT&T Corporation, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Jeffrey Plank

Jeffrey Plank
Task Force Officer
Federal Bureau of Investigation

Subscribed and sworn to before me on January 31, 2024

Daphne A. Oberg

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

Records and information associated with communications to and from the following cellular antenna towers ("cell towers") on the identified dates and timeframes that are within the possession, custody, or control of AT&T Corporation, Verizon Wireless, and T-Mobile US, Inc.

Cell Tower	Dates	Mountain Standard Time
The cell tower(s) that provided cellular service to 4600 S Redwood Rd, Salt Lake City, UT	02/6/2024	Time: 0900-1410 MST
The cell tower(s) that provided cellular service to 351 W Center St, Cedar City, UT	2/8/2024	Time: 1616-1812 MST

***The aforementioned accounts will be referred to as the "Target Accounts" on Attachment B.**

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by the providers.

For the cell towers described in Attachment A, the cellular service providers identified in Attachment A are required to disclose to the United States records and other information (not including the contents of communications) about all communications made using the cell tower(s) identified in Attachment A during the corresponding timeframe(s) listed in Attachment A, including records that identify:

A. The telephone call number and unique identifiers for each wireless device in the vicinity of the cell tower ("the locally served wireless device") that registered with the cell tower, including Electronic Serial Numbers (ESN), Mobile Electronic Identity Numbers (MEIN), Mobile Identification Numbers (MIN), Subscriber Identity Modules (SIM), Mobile Subscriber Integrated Services Digital Network Numbers (MSISDN), International Mobile Subscriber Identifiers (IMSI), and International Mobile Equipment Identities (IMEI).
B. For each communication, the "sector(s)" (i.e. the face(s) of the tower(s) that received a radio signal from the locally served wireless device; and
C. The date, time, and duration of each communication.

These records should include records about communications that were initiated before or terminated after the timeframes identified in Attachment A if some part of the communication occurred during the relevant timeframes listed in Attachment A.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 1030 (computer fraud) and 18 U.S.C. § 2113(b) (bank fraud).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted

by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Verizon, AT&T and T-Mobile and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Verizon, AT&T and T-Mobile. The attached records consist of _____ [**GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)**]. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Verizon, AT&T and T-Mobile, and they were made by Verizon, AT&T and T-Mobile as a regular practice; and

b. such records were generated by Verizon, AT&T, T-Mobile's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Verizon, AT&T and T-Mobile in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Verizon, AT&T, T-Mobile, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature